UNITED STATES PATENT AND TRADEMARK OFFICE MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,156	07/14/2003	Seth Jerome Robertson	61164-0003	9506

9629 7590 07/06/2007

MORGAN LEWIS & BOCKIUS LLP
1111 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20004

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
07/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/620,156	ROBERTSON ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) *1,2 and 13-18* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 July 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The election of 4/18/2007 was received and considered.

2. Claims 1-18 are pending.

Election/Restrictions

3. Applicant's election of Invention II in the reply filed on 4/18/2007 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)).

Accordinly, claims 1-2 & 13-18 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 4/18/2007.

Drawings

4. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the figures contain handwritten text that is difficult to read. For example, Fig. 8 includes a box at the top right (when reading the figure) that is difficult to read. Further, Fig. 9 has several note lines that are not labeled. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office

action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

5. The disclosure is objected to because of the following informalities:

a. On p. 1, ¶4, it should be included that application 10/208,402 has issued as patent number 7,162,741.

b. On p. 2 of the specification, sections 8-9 do not include application numbers or filing dates.

Appropriate correction is required.

Claim Objections

6. Claims 6, 9 & 12 are objected to because of the following informalities:

c. Regarding claim 6, "generation of" (line 1) should be replaced with "generating".

d. Regarding claim 6, "the number of attackers" (line 5) should be replaced with "a number of attackers".

e. Regarding claim 6, "the number of attacks per unit time" (line 6) should be replaced with "a number of attacks per unit time".

f. Regarding claim 6, "the percentage" (line 7) should be replaced with "a percentage".

g. Regarding claim 6, "the breakdown " (line 8) should be replaced with "a breakdown".

h. Regarding claim 6, "the temporal" (line 10) should be replaced with "temporal".

i. Regarding claim 9, "generation of" (line 1) should be replaced with "generating".

j. Regarding claim 9, "the number of attackers" (line 6) should be replaced with "a number of attackers".

k. Regarding claim 9, "the number of attacks per unit time" (line 7) should be replaced with "a number of attacks per unit time".

l. Regarding claim 9, "the percentage" (line 8) should be replaced with "a percentage".

m. Regarding claim 9, "the breakdown " (line 9) should be replaced with "a breakdown".

n. Regarding claim 9, "the temporal" (line 11) should be replaced with "temporal".

o. Regarding claim 12, "generation of" (line 1) should be replaced with "generating".

p. Regarding claim 12, "the number of attackers" (line 6) should be replaced with "a number of attackers".

q. Regarding claim 12, "the number of attacks per unit time" (line 7) should be replaced with "a number of attacks per unit time".

r. Regarding claim 12, "the percentage" (line 8) should be replaced with "a percentage".

s. Regarding claim 12, "the breakdown " (line 9) should be replaced with "a breakdown".

t. Regarding claim 12, "the temporal" (line 11) should be replaced with "temporal".

7. Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 3-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

u. Regarding claim 3, the limitation "the two addresses" (line 8) lacks sufficient antecedent basis; for the purposes of this action, the above limitation is understood to read "two addresses".

v. Regarding claim 3, the limitation "similar flags" (line 11) renders the claim vague and indefinite; it is unclear what makes a flag similar to another (term of degree).

w. Regarding claim 3, the claim is vague and indefinite because it is unclear if "similar characteristics" (lines 12-13) is limiting "packets" or "addresses".

x. Regarding claim 3, the limitation "similar flags" (lines 12-13) renders the claim vague and indefinite; it is unclear what makes packets/addresses similar to one another (term of degree).

y. Regarding claim 4, the limitation "said extrapolated network connections" (line 2) lacks sufficient antecedent basis.

z. Regarding claim 4, the limitation "related" (line 5) renders the claim vague and indefinite; it is unclear what makes addresses related (term of degree).

aa. Regarding claim 4, the limitation "each group" (line 6) lacks sufficient antecedent basis; it appears that a group results from the grouping (line 5) and therefore it is understood that of the list of alternatives ("one or more of the following") presented in lines 5+ of the claim, the grouping and scoring steps are part of the same step.

bb. Regarding claim 4, the limitation "the quantity of attack destinations" lacks sufficient antecedent basis; the above limitation is understood to read "a quantity of attack destinations".

cc. Regarding claim 4, the limitation "each group" (line 7) lacks sufficient antecedent basis; it appears that a group results from the grouping (line 5) and therefore it is understood that of the list of alternatives ("one or more of the following") presented in lines 5+ of the claim, the grouping, scoring and generating steps are part of the same step.

dd. Regarding claim 4, the limitation "unusual" (line 9) renders the claim vague and indefinite; "unusual" is a term of degree and therefore its metes and bounds are indefinite.

ee. Regarding claim 4, the limitation "unusually" (line 17) renders the claim vague and indefinite; "unusually" is a term of degree and therefore its metes and bounds are indefinite.

ff. Regarding claim 4, the limitation "the source to the destination" (lines 19-20) lacks sufficient antecedent basis; however since packets are known to have a source and destination associated with them, this is understood to read "a source to a destination."

gg. Regarding claim 4, the limitation "the destination to the source" (lines 21-22) lacks sufficient antecedent basis; however since packets are known to have a source and destination associated with them, this is understood to read "a destination to a source."

hh. Regarding claim 5, the limitation "the control of" (line 1) does not appear to be a method step; for the purposes of this action, the above limitation is read as "controlling".

ii. Regarding claim 8, the limitation "the control of" (line 1) does not appear to be a method step; for the purposes of this action, the above limitation is read as "controlling".

jj. Regarding claim 11, the limitation "the control of" (line 1) does not appear to be a method step; for the purposes of this action, the above limitation is read as "controlling".

10. Regarding the above 35 U.S.C. §112 rejections, any claim rejected but not specifically mentioned is rejected based on its depending from a rejected claim. Further, all claims rejected below under 35 U.S.C. §102 and/or §103 are rejected as best understood.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claim 3 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

kk. Regarding claim 3, the method claim appears to have no concrete and tangible result; the steps of the claim appear to be performing a grouping of data and hence not producing a concrete and tangible result.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claims 3-4 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,453,345 to Trcka et al. (**Trcka**).

Regarding claim 3, Trcka discloses receiving a plurality of messages (traffic, col. 5, lines 25-27) from a data sensor (monitor computer, col. 5, line 30 & col. 6, lines 1-4) located at a

network audit point (network monitoring point, col. 6, lines 1-4 & Fig. 1), each of said messages (traffic) describing an event (transaction, col. 5, lines 41-43) occurring on said communications network (col. 5, lines 41-43), processing one or more of said messages comprising one or more of the following: clustering packets exchanged between the two addresses within a specified time period, clustering packets exchanged between two addresses having certain flags set, clustering packets exchanged between two addresses having similar flags set and clustering packets exchanged between two addresses having similar characteristics (search for all packets containing a particular set of source and destination addresses and containing a particular pattern/similar characteristics, col. 18, lines 39-45).

Regarding claim 4, Trcka discloses processing of one or more extrapolated network connections to produce a detected surveillance probe comprising identifying unusual packets (user may then zoom in on a particular packet to view specific packet or transaction details, col. 18, lines 45-46).

15. Claims 3-4, 6-7 & 9 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,279,113 to Vaidya et al. (**Vaidya**).

Regarding claim 3, Vaidya discloses receiving a plurality of messages (data packets, col. 6, lines 57-59) from a data sensor (data collector, col. 6, lines 57-59) at a network audit point (network segment, col. 6, lines 57-59 & Fig. 1, #10), each of the messages describing an even occurring on said communications network (packets addressed to network objects on the network segment, col. 6, lines 57-59), processing one or more of said messages comprising one

or more of the following: clustering packets exchanged between two addresses having similar characteristics (packets clustered in session application Y and then the instructions on run on those packets, col. 8, lines 21-25).

Regarding claim 4, Vaidya discloses processing one or more extrapolated network connections (session for application Y, col. 8, lines 21-25) to produce a detected surveillance probe (entry into state cache, col. 7, lines 62-64), said processing of one or more said extrapolated network connections to produce a detected surveillance probe comprising one or more of the following : identifying unusual packets (packets from user Z trying to access application Y when not authorized, col. 7, lines 36-41).

Regarding claim 6, Vaidya discloses generating a profile of surveillance activity (counter, col. 8, lines 30-31), said profile of surveillance activity comprising one or more of the following: the number of attacks per unit time/the temporal frequency trends of individual attacker (Z trying to access A) (event occurring a threshold number of times within a predetermined time interval, col. 8, lines 16-21).

Regarding claim 7, Vaidya discloses processing one or more said detected surveillance probes to produce a detected surveillance scan (user Z making access request for file A, col. 8, lines 21-24), said processing of one or more said detected surveillance probes to produce a detected surveillance scan comprising one or more of the following: modeling and detecting surveillance scans performed by a particular source (user Z, col. 7, lines 36-39 & col. 8, lines 26-28) by identifying a source address (user Z) that generates more than a specified number of probes (threshold) within a specified time period (10 minutes, col. 8, lines 21-28).

Regarding claim 9, Vaidya discloses generating a profile of surveillance activity (counter, col. 8, lines 30-31), said profile of surveillance activity comprising one or more of the following: the number of attacks per unit time/the temporal frequency trends of individual attacker (Z trying to access A) (event occurring a threshold number of times within a predetermined time interval, col. 8, lines 16-21).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 5 & 8, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya, as applied to claims 4 & 7 above, in view of U.S. Patent Application Publication 2003/0188189 to Desai et al. (**Desai**).

Regarding claim 5, Vaidya lacks controlling false positive detections versus false negative detections. However, Desai teaches an intrusion detection system that establishes an intrusion by comparing various activities to thresholds and as such teaches that adjusting pre-tuned thresholds improves accuracy and reduces the number of false positives (¶60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Vaidya to include a mechanism for adjusting the metrics used to determine intrusions (such as an intrusion rate of col. 8, lines 16-39). One of ordinary skill in the art would

have been motivated to perform such a modification to reduce the number of false positives, as taught by Desai (¶60).

Regarding claim 8, Vaidya lacks controlling false positive detections versus false negative detections. However, Desai teaches an intrusion detection system that establishes an intrusion by comparing various activities to thresholds and as such teaches that adjusting pre-tuned thresholds improves accuracy and reduces the number of false positives (¶60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Vaidya to include a mechanism for adjusting the metrics used to determine intrusions (such as an intrusion rate of col. 8, lines 16-39). One of ordinary skill in the art would have been motivated to perform such a modification to reduce the number of false positives, as taught by Desai (¶60).

18. Claim 10, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over **Vaidya**, as applied to claim 7 above, in view of U.S. Patent 7,120,931 to **Cheriton** and U.S. Patent 6,424,654 to **Daizo**.

Regarding claim 10, Vaidya lacks grouping of scanning hosts comprising modeling and detecting scans distributed across a series of source addresses by grouping addresses, said grouping being performed by subtracting one address from another and placing the two addresses in the same group if the difference is less than a specified amount. However, Cheriton teaches an intrusion detection system that detects potentially harmful traffic (col. 7, lines 44-52) where the detection causes filtering of traffic from an IP address range; upon

further investigation, the IP address range can be limited to a more narrow range (col. 7, lines 53-57). This allows the remediation of a potentially harmful attack and later limiting filtering only to confirmed destructive packets (col. 7, lines 9-24). This section also describes how the flow analyzer will cause filtering of all packets from, for example, an ISP suspected of hosting an attacker and once the attacker is identified, only analyzing and filtering packets from the attacker. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Vaidya to process surveillance scans (detected unusual traffic) to detect a group of scanning hosts by grouping addresses (i.e. detecting traffic from a broad IP address range, such as an ISP). One of ordinary skill in the art would have been motivated to perform such a modification to filter packets coming from an attacker's host and later limit the filtering to an individual attacker, as taught by Cheriton. As modified, Vaidya lacks subtracting one address from another and placing the two addresses in the same group if the difference is less than a specified amount. However, Daizo teaches that a client can be limited to a single DHCP server because a DHCP server is known to give out a certain range of IP addresses (col. 5, lines 22-27). The client has a reference address and subtracts from the reference address received IP addresses from different DHCP servers; the address with the smallest distance from the reference is the correct DHCP server (col. 5, lines 27-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Vaidya, as modified by Cheriton, to perform the grouping of addresses by subtracting a received IP address from one IP addresses of detected potentially harmful traffic and if it is within a certain range (such as the range described in Cheriton, col. 7, lines 49-56),

grouping two the together. One of ordinary skill in the art would have been motivated to perform such a modification to determine if an IP address is within a certain range and hence to detect and filter all potentially harmful traffic from an ISP using a simple arithmetic method, as taught by Daizo (col. 2, lines 57-59).

19. Claims 11-12, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Vaidya**, **Cheriton** and **Daizo**, as applied to claim 10 above, in further view of **Desai**.

Regarding claim 11, Vaidya, as modified above, lacks controlling false positive detections versus false negative detections. However, Desai teaches an intrusion detection system that establishes an intrusion by comparing various activities to thresholds and as such teaches that adjusting pre-tuned thresholds improves accuracy and reduces the number of false positives (¶60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Vaidya to include a mechanism for adjusting the metrics used to determine intrusions (such as an intrusion rate of col. 8, lines 16-39). One of ordinary skill in the art would have been motivated to perform such a modification to reduce the number of false positives, as taught by Desai (¶60).

Regarding claim 12, Vaidya, as modified above, discloses generating a profile of surveillance activity (counter, col. 8, lines 30-31), said profile of surveillance activity comprising one or more of the following: the number of attacks per unit time/the temporal frequency

trends of individual attacker (Z trying to access A) (event occurring a threshold number of times within a predetermined time interval, col. 8, lines 16-21).

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

ll. U.S. Patent Application Publication 2002/0035683 to Kaashoek et al. is cited for teaching an intrusion detection system that uses (among other things) packet ratios (¶¶56-57) and the number of packets to which there is no response (¶¶61-65).

mm. U.S. Patent 6,301,668 to Gleichauf et al. is cited for teaching an intrusion detection system that prioritizes vulnerability assessment.

nn. U.S. Patent 5,991,881 to Conklin et al. is cited for teaching an intrusion detection system that looks for characteristics, such as the number and types of packets and common source/destination combinations.

oo. U.S. Patent 7,203,963 to Wu et al. is cited for teaching an network traffic classification system that groups traffic into bins (cols. 5-6) by separating IP addresses by the first digits (beginning of col. 5).

pp. U.S. Patent Application Publication 2003/0226038 to Raanan et al. is cited for teaching adaptive security methods for reducing false negatives (¶28).

qq. U.S. Patent Application Publication 2004/0025044 to Day is cited for teaching an intrusion detection system that sniffs packets and determines deviation from normal activity exceeding a threshold (¶51).

rr. U.S. Patent 7,181,768 to Ghosh et al. is cited for teaching an intrusion detection system for reducing false positives/negatives (brief summary).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael J. Simitoski
/Michael J. Simitoski/
June 27, 2007